UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/041,964	01/09/2002	Makoto Oka	SON-2320	4260

7590 01/15/2010

RADER, FISHMAN & GRAUER, P.L.L.C.
Suite 501
1233 20th Street, NW
Washington, DC 20036

EXAMINER	
POWERS, WILLIAM S	
ART UNIT	PAPER NUMBER
2434	

MAIL DATE	DELIVERY MODE
01/15/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte MAKOTO OKA, YOSHIHITO ISHIBASHI,
SHINAKO MASTUYAMA, and HIDEAKI WATANABE

Appeal 2009-001321
Application 10/041,964[1]
Technology Center 2400

Decided: January 15, 2010

Before HOWARD B. BLANKENSHIP, JEAN R. HOMERE, and
JAMES R. HUGHES, *Administrative Patent Judges*.

HOMERE, *Administrative Patent Judge*.

DECISION ON APPEAL

---

[1] Filed on January 9, 2002. This application claims foreign priority to P2001-002220, which was filed January 10, 2001. The real party in interest is Sony Corp.

I. STATEMENT OF THE CASE

Appellants appeal under 35 U.S.C. § 134(a) (2002) from the Examiner's final rejection of claims 1 through 36. (App. Br. 2.)[2] We have jurisdiction under 35 U.S.C. § 6(b) (2008).

We affirm.

Appellants' Invention

Appellants invented a public key certificate issuing system and method, a digital certification apparatus, and a program storage medium for allowing a single certificate authority ("CA") to support a plurality of encryption algorithms. (Spec. 10, l. 24 - 11, l. 8.) According to Appellants, the claimed invention issues a public key certificate with signatures in different algorithms so that devices compatible with a particular encryption algorithm may effectively utilize the public key certificate from one another for cross-certification and data communication therebetween. (Spec. 11, ll. 8-14.)

Illustrative Claim

Independent claim 1 further illustrates the invention as follows:

> 1. A public key certificate issuing system comprising:
> a certificate authority for issuing a public key certificate used by an entity; and
> a registration authority which, on receiving a public key certificate issuance request from any one of entities under jurisdiction thereof, transmits the received request to said certificate authority;
> wherein said certificate authority, having a plurality of signature modules each executing a different encryption algorithm, selects at least one of said plurality of signature

[2] All references to the Appeal Brief are to the Appeal Brief filed on September 4, 2007, which replaced the prior Appeal Brief filed on July 16, 2007.

> modules in accordance with said public key certificate issuance request from said registration authority based upon an identification of an assigned encryption algorithm, said identification of the assigned algorithm being made with reference to a table that associates the registration authority with the assigned encryption algorithm, and causes the selected signature module to attach a digital signature to message data constituting a public key certificate.

Prior Art Relied Upon

The Examiner relies on the following prior art as evidence of unpatentability:

Vaeth	6,035,402	Mar. 7, 2000
Brownlie	6,202,157 B1	Mar. 13, 2001 (filed Dec. 8, 1997)
Boeyen	6,675,296 B1	Jan. 6, 2004 (filed Jun. 28, 1999)

Dan Boneh et al., *On the Importance of Checking Cryptographic Protocols for Faults*, Advances in Cryptology – EUROCRYPT '97, LNCES 1233, 37-51 (W. Furny ed. 1997) (hereinafter "Boneh").

Rejections on Appeal

The Examiner rejects the claims on appeal as follows:

Claims 1 through 3, 5, 6, 9, 10, 12 through 17, 19, 20, 22 through 25, 27, 28, 31, 32, and 34 through 36 stand rejected under 35 U.S.C. § 102(b) as being anticipated by Vaeth.

Claims 4, 7, 26, and 29 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over the combination of Vaeth and Brownlie.

Claims 8, 18, and 30 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over the combination of Vaeth and Boneh.

Claims 11, 21, and 33 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over the combination of Vaeth and Boeyen.

Appellants' Contentions

Appellants contend that Vaeth discloses that the CA produces each type of certificate based on the association between certificate types and requesting entities. (App. Br. 9-11; Reply Br. 3-9.) Therefore, Appellants argue that Vaeth does not teach an association between the registration authority ("RA") used to make a given certificate request and the type of certificates issued by the CA. (*Id.*) Further, Appellants contend that Vaeth's CA only executes crypto cards associated with a given entity to produce a given certificate and, therefore, does not teach that the applicable crypto card is based on an RA associated with a given requesting entity. (*Id.*) Therefore, Appellants' allege that since Vaeth does not associate public key certificates with particular RAs, Vaeth does not teach "a table that associates the registration authority with the assigned encryption algorithm," as recited in independent claim 1. (*Id.*)

Examiner's Findings and Conclusions

The Examiner finds that Vaeth's disclosure of RAs acting as "virtual CAs," whereby each RA causes the CA to apply the appropriate digital signature executed by the various crypto cards, teaches that the applicable crypto cards are based on an RA associated with a given requesting entity. (Ans. 15-16.) Further, the Examiner finds that Vaeth's disclosure of the CA utilizing a different RA, which acts as a "virtual CA" and uses a different crypto card, teaches an association between a RA and a signature algorithm. (*Id.*) Thus, the Examiner finds that Vaeth's disclosure teaches the disputed limitation.

II. ISSUE

Have Appellants shown that the Examiner erred in finding that Vaeth anticipates independent claim 1? In particular, the issue turns on whether Vaeth teaches "a table that associates the registration authority with the assigned encryption algorithm," as recited in independent claim 1.

III. FINDINGS OF FACT

The following Findings of Fact ("FF") are shown by a preponderance of the evidence.

Vaeth

1. Vaeth generally relates to a method and system for "creating and administering certificates digitally signed by a trusted entity[, or CA,] to ensure that certified transactions are authenticated as part of a particular entity." (Abst.) Vaeth Figure 3 depicts a CA facility (190) with on-line computer system (220), RA computers or computer systems (180, 188), and requesters or user computers (170, 177, 178). (Col. 7, ll. 19-32.) In particular, CA system (220) implements procedures in software through generic certificate request server application functions (221) and specialized functions for cardholders (222), merchants (223), and payment gateways (224). (*Id.* at ll. 36-41.) "Each set of functions may have associated 'crypto cards' (246), (247), (248), and (249), respectively, inserted in card reader (245), which perform the cryptographic aspects of their respective functions, including the generation of the particular type of certificate, which in turn includes the encryption of the digital signature of the "virtual CA" relative to that type of certificate." (*Id.* at ll. 41-47.)

2. Vaeth's Figure 4 depicts that a requester (170) may access a certificate request web page at a site maintained by the RA (180), and a link (HTTP or "hyper link") then sends the requester to the certificate request page at the CA-maintained site. (*Id.* at ll. 59-63.) In selection step (403), the requestor (170) selects the option to request a certificate. (*Id.* at ll. 66-67.) The "CA response (404) presents the requester with a Hyper Text Mark Up language ("HTML") form to complete with information for verification against registration data held at RA registration database (181)." (Col. 7, l. 67 - col. 8, l. 3.) The information required on the certification request data form is determined by the RA (180) as the "virtual" CA, but the form is held and distributed from the CA facility (190). (Col. 8, ll. 3-6.) "In request step (406), the requester (170) completes the request form, adds his public key (generated along with a private key), and sends this certificate request and data ("CRD") to CA (190)." (*Id.* at ll. 7-10.)

3. Vaeth discloses that approval for each different type of certificate might be performed by the same RA (180), for example the credit card issuer, acting as a different "virtual CA" (using a different crypto card) for each type of certificate. (Col. 9, ll. 5-9.) "The same CA (190), with software modification of some of its screening functions, can support a different brand of credit card with a different RA acting as a different "virtual CA" using a different crypto card." (*Id.* at ll. 9-12.)

IV. PRINCIPLES OF LAW

Anticipation

In rejecting claims under 35 U.S.C. § 102, "[a] single prior art reference that discloses, either expressly or inherently, each limitation of a

claim invalidates that claim by anticipation." *Perricone v. Medicis Pharm. Corp.*, 432 F.3d 1368, 1375 (Fed. Cir. 2005) (citing *Minn. Mining & Mfg. Co. v. Johnson & Johnson Orthopaedics, Inc.*, 976 F.2d 1559, 1565 (Fed. Cir. 1992)).

> Anticipation of a patent claim requires a finding that the claim at issue "reads on" a prior art reference. In other words, if granting patent protection on the disputed claim would allow the patentee to exclude the public from practicing the prior art, then that claim is anticipated, regardless of whether it also covers subject matter not in the prior art.

Atlas Powder Co. v. IRECO, Inc., 190 F.3d 1342, 1346 (Fed Cir. 1999) (internal citations omitted).

V. ANALYSIS

35 U.S.C. §102(b) Rejection

Claim 1

Independent claim 1 recites, in relevant part, "a table that associates the registration authority with the assigned encryption algorithm."

As detailed in the Findings of Fact section above, Vaeth discloses creating and administering digital certificates utilizing a CA facility via a RA and corresponding requester. (FF 1.) The CA system issues certificates based on generic certificate request server application functions associated with respective crypto cards. (*Id.*) Each crypto card generates a particular type of certificate, which also includes the encryption of the digital signature relative to the respective certificate. (*Id.*) We find that Vaeth's disclosure teaches that the CA issues certificates by utilizing different types of crypto cards which execute different encryption algorithms.

Further, Vaeth discloses that when a certificate is requested, the form completed by the requestor is verified against registration data held in a RA database. (FF 2.) The CA system can support different RAs that support different entities which utilize different crypto cards. (FF 3.) We find that Vaeth's disclosure of an RA database teaches a table that indexes RAs. We also find that Vaeth's disclosure teaches that different RAs are capable of being associated with different crypto cards. In summary, we find that Vaeth's disclosure teaches a CA that issues certificates by referencing a table that indexes RAs in order to identify the corresponding crypto card and execute the relevant encryption algorithm. Thus, we find the Vaeth's cited disclosure teaches the disputed limitation. It follows that Appellants have not shown that the Examiner erred in finding that Vaeth anticipates independent claim 1.

Claims 2, 3, 9, 10, 12 through 17, 19, 20, 22 through 25, 31, 32, and 34 through 36

Appellants do not provide separate arguments with respect to claims 2, 3, 9, 10, 12 through 17, 19, 20, 22 through 25, 31, 32, and 34 through 36. Therefore, we select independent claim 1 as representative of the cited claims. Consequently, Appellants have not shown error in the Examiner's rejection of claims 2, 3, 9, 10, 12 through 17, 19, 20, 22 through 25, 31, 32, and 34 through 36 for the reasons set forth in our discussion of independent claim 1. 37 C.F.R. § 41.37(c)(1)(vii).

Claims 5 and 27

Appellants contend that Vaeth's disclosure of a given entity making a request through different RAs does not teach that the type of certificate issued by the CA is based on the RA authenticating a given entity. (App. Br.

11-12; Reply Br. 9.) Further, Appellants allege that claim 5 depends from claim 3 and, therefore, entails "a[n] encryption algorithm specific to each of said registration authorities," or a one-to-one relationship between signatures and RAs. (Reply Br. 10.) Thus, Appellants argue that Vaeth's cited disclosure does not teach "wherein said registration authority management data includes signature module identification information applicable to signatures," as recited in dependent claim 5. We do not agree.

As detailed in the Findings of Fact section above, Vaeth discloses that the requester accesses a hyperlink maintained by the RA. (FF 2.) Upon selecting the option to request a certificate, the RA acts as a "virtual" CA by determining the information required on the certificate request form. (*Id.*) Once the certificate request form is complete, the RA sends the CRD to the CA. (*Id.*) We find that Vaeth's disclosure of the RA acting as a "virtual" CA teaches that the RA is capable of determining data that is applicable to the corresponding crypto card and relevant encryption algorithm. We also find that Vaeth's disclosure teaches that the RA transmits the certificate request and corresponding data to the CA. In summary, we find that Vaeth's disclosure teaches that the RA determines and transmits a certificate request and respective data to the CA which allows the CA to identify the corresponding crypto card and execute the relevant encryption algorithm. Thus, we find that Vaeth's cited disclosure teaches the disputed limitation.

Additionally, we note that Appellants cannot rely solely upon the content of the RA management data to patentably distinguish dependent claim 5 over the prior art of record. The content of such data is non-functional descriptive material, and it is therefore not entitled to any patentable weight. *See In re Lowry*, 32 F.3d 1579, 1583 (Fed. Cir. 1994)

("Lowry does not claim merely the information content of a memory…. Nor does he seek to patent the content of information resident in a database."). *See also Ex parte Nehls*, 88 USPQ2d 1883, 1887-90 (BPAI 2008) (precedential); *Ex parte Curry*, 84 USPQ2d 1272 (BPAI 2005) (informative), aff'd, slip op. 06-1003 (Fed. Cir. June 2006) (Rule 36). It follows that Appellants have not shown that the Examiner erred in finding that Vaeth anticipates dependent claim 5.

Appellants do not provide separate arguments with respect to dependent claim 27. Therefore, we select dependent claim 5 as representative of the cited claim. Consequently, Appellants have not shown error in the Examiner's rejection of dependent claim 27 for the reasons set forth in our discussion of dependent claim 5. 37 C.F.R. § 41.37(c)(1)(vii).

Claim 6

Appellants contend that Vaeth's disclosure of utilizing an RA to decide which entity is authorized to make a certificate request does not teach that the authorization includes encryption algorithm designation information. (App. Br. 12; Reply Br. 10-11.) Therefore, Appellants allege that Vaeth does not teach "wherein said registration authority transmits encryption algorithm designation information along with said public key certificate issuance request to said certificate authority," as recited in dependent claim 6. We do not agree.

As set forth above, we find that Vaeth's disclosure teaches that the RA determines and transmits a certificate request and respective data to the CA. Thus, we find that Vaeth's disclosure teaches the disputed limitation. It follows that Appellants have not shown that the Examiner erred in finding that Vaeth anticipates dependent claim 6.

Claim 28

Appellants contend that Vaeth does not use information from a respective RA to determine which encryption algorithm to use to produce a given type of certificate. (App. Br. 14.) Further, Appellants allege that Vaeth's RAs simply provide verification of the CRD and relay information from an entity to the CA. (Reply Br. 15.) Therefore, Appellants argue that Vaeth does not teach " wherein said digital certification apparatus, based on encryption designation information received along with said public key issuance request, selects a signature module applicable to the designated encryption algorithm," as recited in dependent claim 28. We do not agree.

As set forth above, we find that Vaeth's disclosure teaches that the CA receives a certificate request and respective data from the RA, whereby the CA identifies the corresponding crypto card and executes the relevant encryption algorithm. Thus, we find that Vaeth's disclosure teaches the disputed limitation. It follows that Appellants have not shown that the Examiner erred in finding that Vaeth anticipates dependent claim 28.

35 U.S.C. §103(a) Rejection

Claims 4, 7, 8, 11, 18, 21, 26, 29, 30, and 33

Appellants do not provide separate arguments with respect to dependent claims 4, 7, 8, 11, 18, 21, 26, 29, 30, and 33. Therefore, we select independent claim 1 as representative of the cited claims. Consequently, Appellants have not shown error in the Examiner's rejection of dependent claims 4, 7, 8, 11, 18, 21, 26, 29, 30, and 33 for the reasons set forth in our discussion of independent claim 1. 37 C.F.R. § 41.37(c)(1)(vii).

VI. CONCLUSIONS OF LAW

1. Appellants have not shown that the Examiner erred in rejecting claims 1 through 3, 5, 6, 9, 10, 12 through 17, 19, 20, 22 through 25, 27, 28, 31, 32, and 34 through 36 as being anticipated under 35 U.S.C. § 102(b).

2. Appellants have not shown that the Examiner erred in rejecting claims 4, 7, 8, 11, 18, 21, 26, 29, 30, and 33 as being unpatentable under 35 U.S.C. § 103(a).

VII. DECISION

1. We affirm the Examiner's decision to reject claims 1 through 3, 5, 6, 9, 10, 12 through 17, 19, 20, 22 through 25, 27, 28, 31, 32, and 34 through 36 under 35 U.S.C. §102(b).

2. We affirm the Examiner's decision to reject claims 4, 7, 8, 11, 18, 21, 26, 29, and 33 under 35 U.S.C. §103(a).

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv) (2009).

AFFIRMED

nhl

RADER, FISHMAN & GRAUER, P.L.L.C.
Suite 501
1233 20th Street NW
Washington, DC 20036